



Daily Open Source Infrastructure Report 22 April 2015

Top Stories

- Check Point Software researchers identified a security hole in unpatched versions of eBay's Magento e-commerce platform that can be exploited to gain access to databases containing customers' financial and personal information. – *Securityweek* (See item [2](#))
- The U.S. Department of Agriculture announced April 20 that about 5.3 million hens at a commercial egg-laying facility in Osceola County, Iowa, must be culled as a precaution after a strain of bird flu was detected in the flock. – *Des Moines Register* (See item [6](#))
- Blue Bell Creameries recalled April 20 all of its products currently on the market in 23 U.S. States and abroad due to an ongoing Listeria outbreak that has sickened at least 10 individuals, including 3 people who died from infection. – *Food Safety News* (See item [7](#))
- An underground cable issue sparked a transformer explosion that damaged the Suburban Building and nearby businesses in Radnor Township, Pennsylvania, April 20, and prompted Philadelphia Electric Company crews to cut power to about 80 customers including 14 businesses. – *Norristown Times Herald* (See item [25](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

Nothing to report

[\[Return to top\]](#)

Chemical Industry Sector

See item [11](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

1. *April 20, Associated Press* – (New Mexico) **DOE says radioactive waste in drums at Los Alamos are stable.** Investigators with the U.S. Department of Energy stated during the week of April 13 that dozens of drums of radioactive waste stored at the Los Alamos National Laboratory in New Mexico were stable after officials observed chemical reactions occurring in containers that were being monitored following a 2014 breach that closed the Waste Isolation Pilot Plant in Carlsbad indefinitely.
Source: <http://www.abqjournal.com/572419/news/doe-says-radioactive-waste-in-drums-at-los-alamos-are-stable.html>

[\[Return to top\]](#)

Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

2. *April 20, Securityweek* – (International) **Malicious hackers can exploit a vulnerability in Magento to access credit card data.** Security researchers at Check Point Software identified a security hole in unpatched versions of eBay's Magento e-commerce platform that contain remote code execution (RCE) vulnerabilities that could allow attackers to execute hypertext preprocessor (PHP) code on Web servers containing online stores in order to gain access to databases containing customers' credit card, financial, and personal information.
Source: <http://www.securityweek.com/critical-flaw-magento-ecommerce-platform->

[exposes-online-shops](#)

For another story, see item [24](#)

[\[Return to top\]](#)

Transportation Systems Sector

3. *April 20, Associated Press* – (Wyoming) **Fiery pileup on I-80 in Wyoming kills 1, closes interstate again.** Interstate 80 in southeast Wyoming was closed for several hours April 20 following a chain-reaction accident that occurred when 2 semi-trucks crashed causing one to jackknife in both westbound lanes. One person was killed and 16 others were injured in the incident that also involved a semi-truck carrying a flammable liquid that caught fire and required foam to put it out.
Source: http://www.denverpost.com/news/ci_27951242/pileup-i-80-kills-1-closes-interstate-again
4. *April 20, Augusta Chronicle* – (Georgia) **U.S. Airways jet bound for Charlotte diverted to Augusta.** A U.S. Airways flight headed to Charlotte, North Carolina, from Tallahassee, Florida, made an emergency landing at Augusta Regional Airport in Georgia, April 20 after the pilot reported a mechanical problem when an indicator light in the jet's cockpit failed. The plane landed safely and the indicator light was repaired while passengers were placed on a different flight to Charlotte several hours later.
Source: <http://chronicle.augusta.com/latest-news/2015-04-20/us-airways-jet-bound-charlotte-diverted-augusta>
5. *April 19, Yavapai County Daily Courier* – (Arizona) **Crash at Highway 69 and Fain Road kills 1.** Highway 69 was shut down in both directions between milepost 284 and the intersection of Fain Road in Prescott Valley for more than 5 hours April 18-April 19 while crews cleared the scene of a head-on collision that killed 1 person and injured a second.
Source:
<http://dcourier.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=144312>

[\[Return to top\]](#)

Food and Agriculture Sector

6. *April 21, Des Moines Register* – (Iowa) **5.3 million Iowa laying hens to be destroyed in bird flu outbreak.** The U.S. Department of Agriculture announced April 20 that about 5.3 million laying hens at an Osceola County commercial egg-laying facility must be culled as a precaution after a strain of bird flu was detected in the flock. More than 2.6 million additional birds have been killed as a result of the bird flu, which has been confirmed at more than 50 sites across at least 8 States, including Wisconsin where a state of emergency was declared over the outbreak.
Source: <http://www.desmoinesregister.com/story/money/agriculture/2015/04/20/avian-flu-chicken-eggs/26094811/>

7. *April 21, Food Safety News* – (International) **CDC Reports Two More Cases in Listeria Outbreak.** Texas-based Blue Bell Creameries issued a voluntary recall April 20 for all of its products currently on the market in 23 U.S. States and abroad due to an ongoing Listeria outbreak that has been connected to several of the company's plants. The U.S. Centers for Disease Control and Prevention reported 2 new cases that are linked to Blue Bell products April 21, increasing the case count to 10, including 3 cases that resulted in death.
Source: <http://www.foodsafetynews.com/2015/04/blue-bell-recalls-all-products-made-in-all-company-facilities>
8. *April 21, U.S. Department of Agriculture* – (National) **Kayem Foods recalls sausage products due to possible foreign matter contamination.** The Food Safety and Inspection Service announced April 20 that Kayem Foods recalled about 59,203 pounds of fully cooked chicken sausage products after the firm received complaints from 2 consumers who found small pieces of plastic in the product. The recalled products were sold under the al fresco and Trader Joe's brand names at retail locations nationwide.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-066-2015-release>
9. *April 20, Los Angeles Times* – (California) **Raw fish linked to Salmonella outbreak in California.** Health officials are investigating the cause of a Salmonella outbreak that has sickened 25 people who reside in or have visited California, with 80 percent of those affected reportedly consuming raw tuna and sushi prior to falling ill. The Salmonella strain associated with the outbreak had not been detected in humans or animals prior to March, posing challenges to the health officials who are investigating.
Source: <http://www.latimes.com/local/lanow/la-me-ln-raw-fish-sushi-linked-to-salmonella-outbreak-in-california-20150420-story.html>
10. *April 20, Associated Press* – (Minnesota) **Another Minnesota turkey farm hit by deadly bird flu strain.** The U.S. Department of Agriculture confirmed April 20 the presence of the H5N2 bird flu virus in a flock of 23,000 turkeys in Kandiyohi County, and reported that about 9,000 turkeys from a separate farm in the county will be culled due to exposure the first flock. Authorities also reported that a backyard flock of 33 mixed birds in Juneau County was affected by the virus, bringing the total number of Minnesota farms connected with the outbreak to 28.
Source: <http://minnesota.cbslocal.com/2015/04/20/another-minnesota-turkey-farm-hit-by-deadly-bird-flu-strain/>
11. *April 20, U.S. Environmental Protection Agency* – (Delaware; Indiana; North Carolina) **Settlements emphasize that pesticides need to be labeled correctly, protecting public and environment from misbranded products.** The U.S. Environmental Protection Agency reached settlements with 3 companies that produce and/or market pesticides to resolve charges that the businesses or their agents sold pesticide products that failed to meet Federal labeling requirements. Bayer CropScience LP of North

Carolina, was issued an \$85,500 penalty; E.I. du Pont de Nemours and Co., of Delaware, was issued a \$22,200 penalty; and Dow AgroSciences LLC of Indiana, was issued a \$182,640 penalty and ordered to implement an environmentally-beneficial project worth about \$231,000.

Source:

<http://yosemite.epa.gov/opa/admpress.nsf/21b8983ffa5d0e4685257dd4006b85e2/17ee5e34bb30775085257e2d00568ad7!OpenDocument>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

12. *April 20, KMA 960 AM Shenandoah/99.1 FM Clarinda* – (Iowa) **Wastewater discharge reported near Audubon.** The Iowa Department of Natural Resources advised April 20 that residents should stay away from Bluegrass Creek for 48 hours after a citywide power outage caused an estimated 200,000 gallons of partially treated wastewater to discharge into the creek near Audubon April 19.

Source: http://www.kmaland.com/news/wastewater-discharge-reported-near-audubon/article_0afaf5de-e78f-11e4-ac4f-0799119ef498.html

[\[Return to top\]](#)

Healthcare and Public Health Sector

13. *April 21, Reuters* – (Indiana) **Indiana governor extends needle program to fight HIV.** The governor of Indiana announced April 20 that an emergency health order, including a needle exchange program, that was set to expire April 24 will be extended for an additional 30 days in response to an ongoing HIV outbreak caused by intravenous drug abuse in the State. Authorities reported that the outbreak has reached 134 confirmed and preliminary cases.

Source: <http://www.msn.com/en-us/news/us/indiana-governor-extends-needle-program-to-fight-hiv/ar-AAboMfl>

[\[Return to top\]](#)

Government Facilities Sector

14. *April 21, Miami Herald* – (Florida) **Nearly 2,000 acres burn in stubborn SW Miami-Dade brush fire.** Crews worked to put out hotspots April 20 that reignited due to shifting wind April 21 after more than 1,850 acres of trees and grass burned in southwest Miami-Dade County, prompting officials to close several streets in the area.

Source: <http://www.miamiherald.com/news/local/community/miami-dade/article19044921.html>

15. *April 21, Mohave Valley Daily News* – (Arizona) **Tote bag prompts evacuation of courthouse.** The Kingman/Cerbat Courthouse in Arizona was evacuated for over 4 hours April 20 due to a suspicious tote bag that was found on the Mohave County

Sheriff's Office property near the courthouse. A bomb squad rendered the tote bag containing unknown objects safe after inspecting it.

Source: http://www.mohavedailynews.com/news/tote-bag-prompts-evacuation-of-courthouse/article_f56f4668-e7fa-11e4-8e92-4bab161f2fcd.html

16. *April 20, Salt Lake City Deseret News* – (Utah) **3 high schoolers suffer minor injuries after buses collide.** Two Box Elder School District buses collided into each other on Interstate 80 near Saltair April 20, leaving 3 high school students with minor injuries. Source: <http://www.deseretnews.com/article/865626882/3-high-schoolers-suffer-minor-injuries-after-buses-collide.html>

17. *April 20, Bucks County Courier Times* – (Pennsylvania) **Power outage closes Wrightstown Elementary School Monday.** Wrightstown Elementary School in Council Rock was closed April 20 due to a power outage caused by heavy rain that damaged a piece of aerial equipment. Source: http://www.buckscountycouriertimes.com/news/local/power-outage-closes-wrightstown-elementary-school-monday/article_f50cd585-79e3-58ea-ae8e-9eafe2173b57.html

[\[Return to top\]](#)

Emergency Services Sector

18. *April 20, Iroquois County's Times-Republic* – (Illinois) **Cut cable wreaks havoc on 911, routine calls.** A cut AT&T fiber optic cable line near Papineau knocked out emergency service calls in Iroquois County April 20. Emergency calls were temporarily rerouted to Kankakee County's Kan-Com while crews spent several hours working to restore services. Source: http://www.newsbug.info/iroquois_countys_times-republic/cut-cable-wreaks-havoc-on-routine-calls/article_5ce763da-e7a5-11e4-86c7-cf94e200e821.html

[\[Return to top\]](#)

Information Technology Sector

19. *April 21, Softpedia* – (International) **Highly popular WordPress plugins vulnerable to XSS attacks.** A security researcher from Scrutinizer discovered an issue with two coding functions used in many content management system (CMS) plugins created by WordPress developers that could allow attackers to run cross-site scripting (XSS) attacks and access sensitive areas of affected Web sites. The vulnerability was a result of improper documentation regarding external users' ability to run commands via the functions. Source: <http://news.softpedia.com/news/At-Least-17-Popular-WordPress-Plugins-Vulnerable-to-XSS-Attacks-478968.shtml>
20. *April 21, Softpedia* – (International) **iOS apps from developers vulnerable to HTTPS data decryption.** Research from SourceDNA revealed that almost 1,000 iOS apps are

vulnerable to a security flaw in build 2.5.1 of open source AFNetworking that disables secure sockets layer (SSL) certificate validation, which could allow attackers to carry out man-in-the-middle (MitM) attacks and read encrypted information in plain text. The flaw was patched in late March, but many developers have not yet integrated the updated code.

Source: <http://news.softpedia.com/news/iOS-Apps-from-Developers-Vulnerable-to-HTTPS-Data-Decryption-478951.shtml>

21. *April 21, Softpedia* – (International) **Fake antivirus delivered to users in the US via Fiesta exploit kit.** Security researchers at Trend Micro discovered that cybercriminals have switched the payload delivered via the Fiesta exploit kit (EK) from crypto-malware such as TeslaCrypt to a fake antivirus program called “Antivirus Pro 2015” that disables Windows tools and software that could deactivate it, before requiring users to pay to remove the infection. Researchers reported that Fiesta EK distributors targeted the U.S. more than any other country in March.
Source: <http://news.softpedia.com/news/Fake-Antivirus-Delivered-to-Users-in-the-US-via-Fiesta-Exploit-Kit-478933.shtml>
22. *April 21, Help Net Security* – (International) **New fileless malware found in the wild.** Security researchers at Trend Micro discovered that a new fileless malware, dubbed Phasebot, uses Microsoft Windows PowerShell to evade detection and run components hidden in the Windows registry, contains an external module loader to add and remove functionalities on infected systems, and can execute numerous routines per the instruction of the bot administrator.
Source: http://www.net-security.org/malware_news.php?id=3021
23. *April 20, Softpedia* – (International) **New ransomware “Threat Finder” delivered by Angler exploit kit.** Security researchers at Rackspace discovered that a new piece of crypto-malware called Threat Finder has been distributed in drive-by attacks via Bedep malware downloaded by the Angler exploit kit (EK). The crypto-malware encrypts important file types including documents, media files, and database formats before asking affected users for bitcoin in exchange for the decryption key.
Source: <http://news.softpedia.com/news/New-Ransomware-Threat-Finder-Delivered-by-Angler-Exploit-Kit-478881.shtml>
24. *April 20, IDG News Service* – (International) **Pushdo spamming botnet gains strength again.** Security researchers at Fidelis Cybersecurity reported that an updated version of the Pushdo botnet has infected systems in over 50 countries with the Fareit and Cutwail malware as well as the Dyre and Zeus banking trojans. The spamming botnet has been in operation since 2007 due to its frequently changing command and control (C&C) system that generates 30 domain names a day that infected computers can contact.
Source: http://www.networkworld.com/article/2912533/pushdo-spamming-botnet-gains-strength-again.html#tk.rss_all

For another story, see item [2](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

See item [18](#)

[\[Return to top\]](#)

Commercial Facilities Sector

25. *April 21, Norristown Times Herald* – (Pennsylvania) **Transformer explosion in Radnor Township shatters, closes storefronts.** An underground cable issue sparked a transformer explosion that shattered windows at the Suburban Building and nearby businesses in Radnor Township April 20, and prompted Philadelphia Electric Company crews to cut power to about 80 customers including 14 businesses. Some businesses remained closed April 21, while crews expected to restore service to all customers later that day.
Source: <http://www.timesherald.com/general-news/20150421/transformer-explosion-in-radnor-township-shatters-closes-storefronts>
26. *April 21, Wilmington News Journal* – (Maryland) **Fire damages Molly's Market near Elkton, Md.** An April 17 fire at the Molly's Market store near Elkton caused an estimated \$150,000 in damage to the structure and its contents. Officials are investigating the cause of the fire that is believed to have started in an office of the 2-story commercial building.
Source: <http://www.delawareonline.com/story/news/local/2015/04/21/fire-damages-mollys-market-near-elkton-md/26116533/>
27. *April 20, KSHB 41 Kansas City* – (Missouri) **Clinton Police Department says no explosive found at WalMart, will continue to investigate.** A Walmart store in Clinton, Missouri, was evacuated and closed for more than 7 hours April 20 while authorities investigated after an individual phoned the store and claimed there was an explosive near the business. The store was cleared to reopen after the Whiteman Air Force Base Explosive Ordinance Disposal team found no explosive device at the scene.
Source: <http://www.kshb.com/news/region-missouri/clinton-police-department-missouri-highway-patrol-investigate-bomb-threat-at-clinton-walmart>
28. *April 19, Associated Press* – (Wyoming) **Fire damages 6 Jackson businesses in strip mall.** Six businesses including a gun shop at a strip mall in Jackson, Wyoming, suffered extensive damage from an April 19 fire that remains under investigation. A

nearby apartment building and hotel were temporarily evacuated as a precaution.
Source: <http://www.localnews8.com/fire-damages-6-jackson-businesses-in-strip-mall/32452548>

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.